NCA Requirements for Company

S/N	Requirement	Remarks
	Cybersecurity Governance	
1.	Cybersecurity strategy/plan for the year	
2.	A cybersecurity department/unit independent from the IT Department	
3.	A CISO (Chief Information Security Officer) and relevant staff, must be filled with experienced Saudi professionals	
4.	A cybersecurity steering committee	
5.	Cybersecurity policies and procedure approved by CEO, and distributed to all staff • Policies must be supported by technical security standards • Policies must be reviewed periodically • Ensuring compliance of policies,	
6.	Cybersecurity roles and responsibilities must be defined and reviewed regularly.	
7.	Cybersecurity risk management methodology and procedures and must be implemented by cybersecurity unit. • Risk management will be implement at the stages i. Early stages of technology projects ii. Before making major changes to technology infrastructure. iii. During the planning phase of obtaining third party service iv. During the planning phase and before going live for new technology products and services.	
8.	The cybersecurity requirements in project and assets (information/technology) change management must include at least the following: • Vulnerability assessment and remediation. • Conducting a configurations' review, secure configuration and hardening and patching before changes or going live for technology projects.	
9.	The cybersecurity requirements related to software and application development projects must include at least the following: • Using secure coding standards. • Using trusted and licensed sources for software development tools and libraries. • Conducting compliance test for software against the defined organizational cybersecurity requirements. • Secure integration between software components.	

	• Conducting a configurations' review, secure configuration and hardening and patching before going live for software products	
10.	Compliance with other cybersecurity regulations	
11.	Periodic Internal Audit to ensure compliance Audit reports to be presented to the cybersecurity steering committee	
12.	Cybersecurity in Human Resources	
13.	Cybersecurity awareness program implemented and reviewed periodically	
14.	Cybersecurity personnel to be sent on trainings on cybersecurity	
Cybersecurity Defense		
1.	Asset management Policy • Asset inventory • Acceptable use policy • Asset classification	
2.	Identity and Access management • Access Control • Privilege access • Remote access(VPN) • Least privilege • Review	
3.	Information systems/ facilities protection • Antivirus • Patch management • Restricted use of external storage • Centralized clock synchronization	
4.	Email Protection	
5.	Network Security The cybersecurity requirements for network security management must include at least the following: • Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles. • Network segregation between production, test and development environments. Secure browsing and Internet connectivity including restrictions on the use of file storage/sharing and remote access websites, and protection against suspicious websites. • Wireless network protection using strong authentication and encryption techniques. • A comprehensive risk assessment and management exercise must be conducted to assess and manage the cyber risks prior to connecting any wireless networks to the organization's internal network.	

	• Management and restrictions on network services, protocols and ports. • Intrusion Prevention Systems (IPS). • Security of Domain Name Service (DNS). • Secure management and protection of Internet browsing channel against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware	
6.	Mobile devices security The cybersecurity requirements for mobile devices security and BYOD must include at least the following: • Separation and encryption of organization's data and information stored on mobile devices and BYODs. • Controlled and restricted use based on job requirements. • Secure wiping of organization's data and information stored on mobile devices and BYOD in cases of device loss, theft or after termination/separation from the organization. • Security awareness for mobile devices users.	
7.	Data Protection The cybersecurity requirements for protecting and handling data and information must include at least the following: • Data and information ownership. • Data and information classification and labeling mechanisms. • Data and information privacy	
8.	Cryptography The cybersecurity requirements for cryptography must include at least the following: • Approved cryptographic solutions standards and its technical and regulatory limitations. • Secure management of cryptographic keys during their lifecycles. • Encryption of data in-transit and at-rest as per classification and related laws and regulations	
9.	Backup and Recovery The cybersecurity requirements for backup and recovery management must include at least the following: • Scope and coverage of backups to cover critical technology and information assets. • Ability to perform quick recovery of data and systems after cybersecurity incidents. • Periodic tests of backup's recovery effectiveness	
10.	Vulnerability Management The cybersecurity requirements for technical vulnerabilities management must include at least the following:	

	• Periodic vulnerabilities assessments. • Vulnerabilities classification based on criticality level. • Vulnerabilities remediation based on classification and associated risk levels. • Security patch management. • Subscription with authorized and trusted cybersecurity resources for up-to-date information and notifications on technical vulnerabilities.	
11.	Penetration Testing The cybersecurity requirements for penetration testing processes must include at least the following: • Scope of penetration tests which must cover Internet-facing services and its technical components including infrastructure, websites, web applications, mobile apps, email and remote access. • Conducting penetration tests periodically	
12.	Cybersecurity event log and Monitoring The cybersecurity requirements for event logs and monitoring management must include at least the following: • Activation of cybersecurity event logs on critical information assets. • Activation of cybersecurity event logs on remote access and privileged user accounts. • Identification of required technologies (e.g., SIEM) for cybersecurity event logs collection. • Continuous monitoring of cybersecurity events. • Retention period for cybersecurity event logs (must be 12 months minimum)	
13.	Cybersecurity threat and Incident management The requirements for cybersecurity incidents and threat management must include at least the following: • Cybersecurity incident response plans and escalation procedures. • Cybersecurity incidents classification. • Cybersecurity incidents reporting to NCA. • Sharing incidents notifications, threat intelligence, breach indicators and reports with NCA. • Collecting and handling threat intelligence feeds.	
14.	Physical security The cybersecurity requirements for physical protection of information and technology assets must include at least the following: • Authorized access to sensitive areas within the organization (e.g., data center, disaster recovery center, sensitive information processing facilities, security surveillance center, network cabinets). • Facility entry/exit records and CCTV monitoring.	

	• Protection of facility entry/exit and surveillance records. Secure destruction and re-use of physical assets that hold classified information (including documents and storage media). • Security of devices and equipment inside and outside the organization's facilities.	
15.	Web Application Security The cybersecurity requirements for external web applications must include at least the following: • Use of web application firewall. • Adoption of the multi-tier architecture principle. • Use of secure protocols (e.g., HTTPS). • Clarification of the secure usage policy for users. • Multi-factor authentication for users' access.	
16.	Business Continuity The cybersecurity requirements for business continuity management must include at least the following: • Ensuring the continuity of cybersecurity systems and procedures. • Developing response plans for cybersecurity incidents that may affect the business continuity. • Developing disaster recovery plans.	
17.	Third-Party Cybersecurity	
18.	Cloud Computing and Hosting Cybersecurity	